Krypto@Informatik11

Codierung und Verschlüsselung

Arbeitsheft zum digitalen Escaperoom

The Mystery of Crypto-Castle

Konzeption des Arbeitsheftes:

Das Arbeitsheft bezieht sich auf den Online-Escaperoom „The Mystery of Cryptocastle“, der das Thema Codierung und Verschlüsselung (Informatik-Lehrplan der 11. Jahrgangsstufe) behandelt.

Dr. Wolfgang Pfeffer

Dominicus-von-Linprun-Gymnasium Viechtach
E-Mail: schule@pfeffer-wolfgang.de

Tobias Fuchs

Universität Passau
E-Mail: fuchs_unipa@outlook.de

1. Überblick

Das Arbeitsheft flankiert den digitalen Escaperoom **The Mystery of Crypto-Castle**, der die Thematik „Codierung und Verschlüsselung“ im Lehrplan der 11. Jahrgangsstufe (NTG) behandelt:

Der Escape-Room wurde mit der Plattform **Genially** erstellt und ermöglicht eine interaktive Erkundung einer verfallenen Burgruine, in der es eine Vielzahl an Rätseln rund um das Thema Codierung und Verschlüsselung zu meistern gilt. Der Escaperoom beinhaltet folgende drei großen Stränge (Bereiche der Burg):

(a) **Der Burghof:** Hier warten Rätsel rund um das Thema *Symmetrische Verschlüsselungen* sowie einfache *Codierungen*.

(b) **Der Burgturm:** Auf dem Weg zum Burgturm warten *Codierungen im Binär- und Hexadezimalsystem* sowie *RGB-Farbdarstellungen*.

(c) **Die Gruft:** In der Gruft warten *Asymmetrische Verschlüsselungsverfahren, Zertifikate und Digitale Signaturen*.

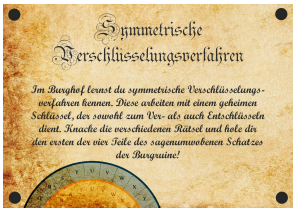
Für jeden erfolgreich absolvierten Strang bekommt man eines von drei Teil-Fragmenten, welche zur Bergung des sagenumwobenen Schatzes benötigt werden. Ist man im Besitz aller drei Teil-Fragmente, kann man sich in der **Höhle im Burgfelsen** auf die Suche nach dem Schatz begeben, wobei man noch Aufgaben zu *Prüfsummen* bewältigen muss.

Dieses **Arbeitsheft** dient zum Festhalten wichtiger Erkenntnisse sowie zur Reflexion der Aufgaben des Online-Escaperooms. Dabei ist es wichtig, im Arbeitsheft immer nur so weit zu blättern, wie man im Escape-Room selber ist. An manchen Stellen wird man zudem auch durch nebenstehendes Symbol davor gewarnt weiterzublättern, um nicht ungewollt Hinweise zu den Rätseln zu erhalten.

Die drei Stränge können unabhängig voneinander gespielt werden und bauen nicht aufeinander auf. Im Arbeitsheft werden die Stränge in der Reihenfolge gemäß obiger Aufführung aufgeführt.

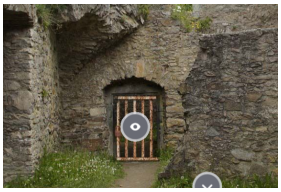
2. Der Burghof – Symmetrische Verschlüsselungsverfahren

Im Burghof lernst du Beispiele von Codierungen sowie symmetrische Verschlüsselungsverfahren kennen. Letztere arbeiten mit einem geheimen Schlüssel, der sowohl zum Ver- als auch Entschlüsseln dient. Knacke die verschiedenen Rätsel und hole dir das erste von drei Code-Fragmenten für den Zugang zum sagenumwobenen Schatz der Burgruine.



Arbeitsauftrag 1: Eisentor im Inneren des Burghofes

Das Eisentor im Inneren des Burghofes ist mit einem rostigen Zahlenschloss versperrt! Finde und kombiniere die Hinweise auf den gesuchten Zahlencode. Notiere deine Entdeckungen hier im Heft:



Blättere erst um, wenn du den Code für das rostige Zahlenschloss gefunden hast!

Überblick (Das Winkeralphabet – Semaphore)

Das **Winkeralphabet** ist ein Verzeichnis von Positionen von zwei identischen Flaggen, die von einer Person gehalten werden. Es dient der optischen Nachrichtenübermittlung z.B. zwischen Schiffen. Beim Winkeralphabet handelt es sich letztlich um eine symbolbasierte **Codierung** des Alphabets.

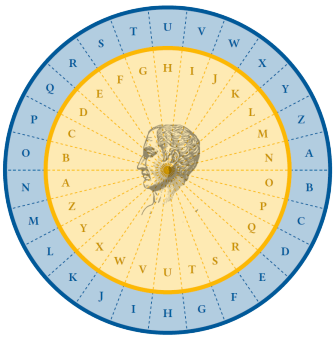
Arbeitsauftrag 2: Der Brunnen

(a) Der Deckel des Brunnens ist mit einem fünfstelligen Buchstabenschloss versperrt. Gelingt es dir, das Schloss zu knacken? Notiere den Code ins Heft und beschreibe, wie du dabei vorgegangen bist. Kommt dir die Person auf dem Schild bekannt vor?

(b) Was hast du im Brunnen entdeckt? Für was könnte der erhaltene Code wohl gut sein?

Blättere erst um, wenn du das Schriftstück im Brunnen entschlüsselt hast!

Überblick (Die Caesar-Verschlüsselung)



Die Caesar-Verschlüsselung, benannt nach Julius Caesar, ist eine der einfachsten und ältesten Formen der Verschlüsselung. Sie ist ein **symmetrisches Verschlüsselungsvefahren**, bei dem jeder Buchstabe im Klartext durch einen Buchstaben mit einem festen Verschiebungswert ersetzt wird. Dieser Verschiebungswert wird oft als „Schlüssel“ bezeichnet. Grundlegend verläuft die Caesar-Verschlüsselung in den folgenden drei Schritten:

(a) **Wählen des Schlüssels**: Der Schlüssel bestimmt, um wie viele Positionen im Alphabet jeder Buchstabe verschoben wird.

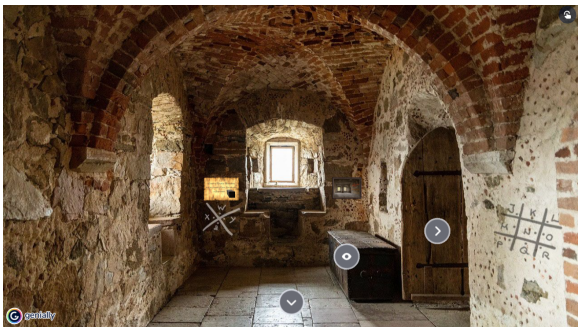
(b) **Verschlüsseln des Klartextes:** Jeder Buchstabe im Klartext wird um den ausgewählten Schlüssel verschoben. Wenn der Schlüssel 3 ist, wird aus dem Buchstaben „A“ ein „D“, aus dem Buchstaben „B“ ein „E“usw.

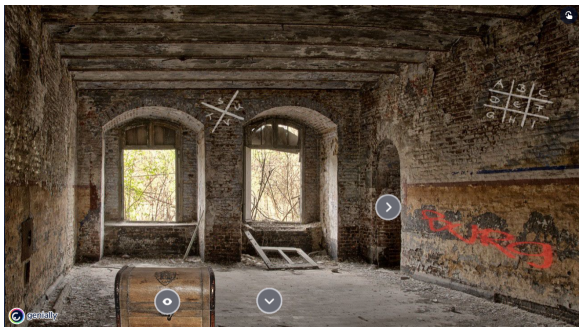
(c) **Entschlüsseln des Geheimtextes:** Um den Geheimtext zurück in den Klartext zu verwandeln, wird der gleiche Schlüssel verwendet (deswegen spricht man auch von einem **symmetrischen Verschlüsselungsverfahren**), jedoch in die entgegengesetzte Richtung.

Die Caesar-Verschlüsselung ist sehr anfällig für Brute-Force-Angriffe und wird aus Sicherheitsgründen selten in der modernen Verschlüsselung eingesetzt.

Arbeitsauftrag 3: Das Gewölbe (Teil 1)

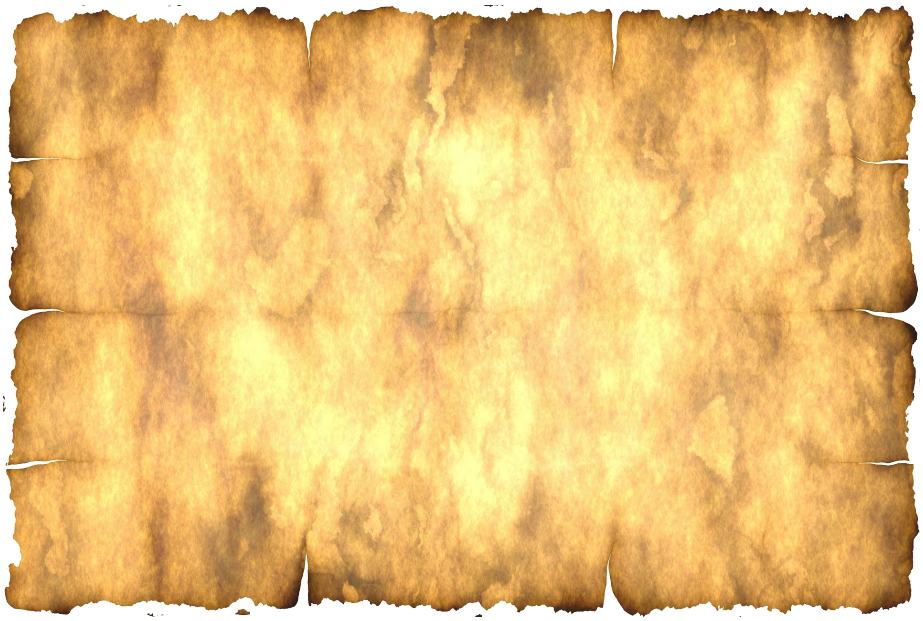
Respekt! Du hast dir Zugang zum Gewölbe verschafft, das an den Burghof angrenzt. Allerdings bist du immer noch einige Schritte von deinem ersten Code-Fragment entfernt!





(a) Hast du dir schon Zugang zu der mysteriösen Holztruhe im ersten Zimmer des Gewölbes verschafft? Erkläre, wie du beim Finden des Codes vorgegangen bist:

(b) In der Truhe entdeckst zu seltsame Schriftzeichen. Was können diese nur bedeuten? Übertrage die Schriftrolle in das Heft und versuche, hinter das Geheimnis der Schriftzeichen zu gelangen. Notiere wieder, wie du hierbei vorgegangen bist.



Blättere erst um, wenn du die geheimen Schriftzeichen entschlüsselt hast!

Überblick (Freimaurer-Alphabet)

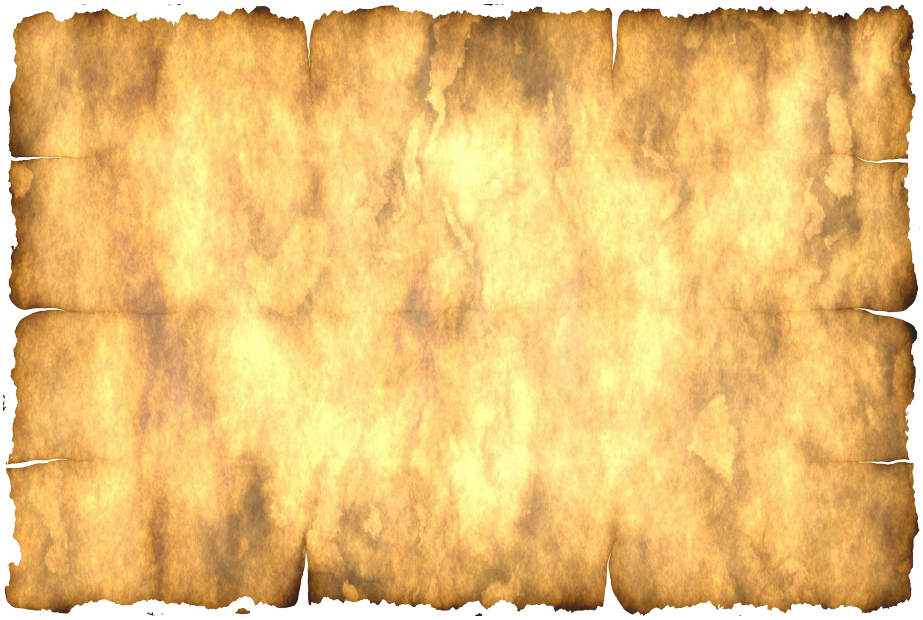
Die Freimaurer sind eine weltweit verbreitete Bruderschaft, die sich auf moralische und ethische Prinzipien konzentriert und sich historischer Rituale und Symbole bedient. Die Ursprünge der Freimaurerei reichen bis ins 18. Jahrhundert zurück. Das **Freimaurer-Alphabet** (oder auch **Freimaurer-Chiffre**) ist ähnlich dem Winkeralphabet eine symbolbasierte **Codierung** des Alphabets. Füllt man die Buchstaben des lateinischen Alphabets wie folgt in die vier kreuzförmigen Gitter, erhält man ein Schema, aus dem man sich das Geheimtextalphabet ableiten kann.

Arbeitsauftrag 4: Das Gewölbe (Teil 2)

(a) In der Truhe findest du ein Beispiel der beschriebenen Verschlüsselung. Notiere die entsprechenden Zeilen hier in Dein Heft und mache dich vertraut, wie die Klartextbuchstaben jeweils verschlüsselt werden. Gelingt es dir auch, vom Geheimtext des Beispiels zurück zum Klartext zu kommen?

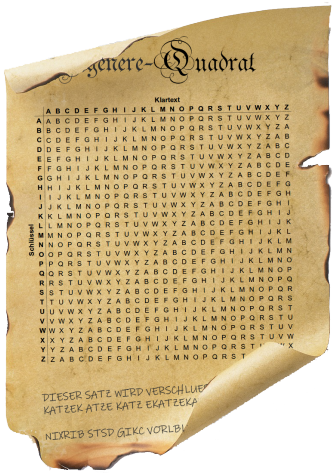
(b) Beschreibe, wie die beschriebene Verschlüsselung funktioniert. Welche Gemeinsamkeiten bzw. Unterschiede gibt es zur Caesar-Verschlüsselung? Welche Verschlüsselung ist einfacher zu knacken und warum?

(c) Übertrage den Geheimtext, den du in der Truhe gefunden hast, in das Heft und entschlüssele den geheimen Code:



Blättere erst um, wenn du den Geheimtext entschlüsselt hast!

Überblick (Die Vigenère-Verschlüsselung)

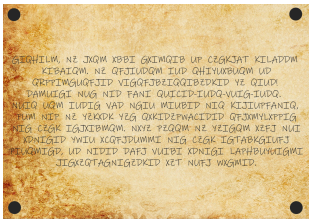


Die **Vigenère-Verschlüsselung** ist eine klassische Verschlüsselungsmethode, die im 16. Jahrhundert entwickelt wurde und nach Blaise de Vigenère, einem französischen Diplomaten und Kryptographen, benannt ist. Diese Methode basiert auf der Verwendung eines Schlüsselworts, um eine Nachricht zu verschlüsseln. Sie gehört (anders als beispielsweise die Caesar-Verschlüsselung) zur Gruppe der **polyalphabetischen Verschlüsselungsmethoden**, was bedeutet, dass ein Klartextbuchstabe nicht stets durch denselben Geheimtextbuchstaben ersetzt wird.

Das grundlegende Konzept der Vigenère-Verschlüsselung besteht darin, jeden Buchstaben der Klartextnachricht basierend auf dem entsprechenden Buchstaben im Schlüsselwort zu verschieben. Dabei wird eine Art verschobenes Alphabet verwendet, das sich basierend auf den Buchstaben im Schlüsselwort ändert. Der Buchstabe `A` im Schlüsselwort entspricht beispielsweise einer Verschiebung von 0 (keine Verschiebung), `B` entspricht einer Verschiebung von 1, `C` einer Verschiebung von 2 und so weiter. Wenn das Ende des Schlüsselworts erreicht ist, wird wieder von vorne begonnen.

Die Vigenère-Verschlüsselung war lange Zeit als sicherer Verschlüsselungsalgorithmus bekannt, bis der britische Kryptograph Charles Babbage im 19. Jahrhundert Methoden entwickelte, um sie zu brechen. Moderne Computer und Kryptoanalysetechniken haben die Vigenère-Verschlüsselung weiterhin anfällig gemacht, wenn das Schlüsselwort nicht sehr lang und zufällig ist. Wie genau man die Vigenère-Verschlüsselung „knacken“ kann, erfährst du hier im Heft, sobald du das letzte Rätsel des Burghofs gemeistert hast.

Arbeitsauftrag 5: Das Gewölbe (Teil 3)



Im letzten Raum des Gewölbes findest du ein Schild mit einem langen Geheimtext. Doch es bringen dich weder die gelernten Entschlüsselungsmethoden der Caesar-Verschlüsselung noch die von Vigenère (mit dem Schlüsselwort `BURG`) weiter:

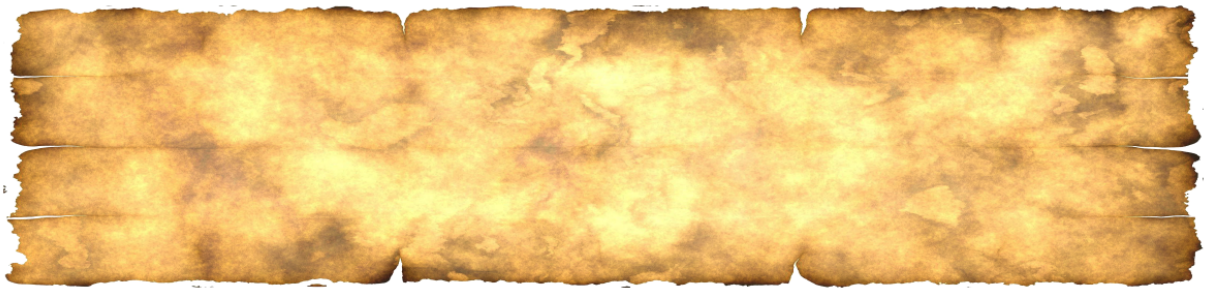
(a) Anders als bei der Caesar-Verschlüsselung wurden die Buchstaben hier in beliebiger Reihenfolge neu zugeordnet. Das Schriftstück in der Schatztruhe verrät dir, wie viele verschiedene Möglichkeiten zur Verschlüsselung sich hieraus ergeben. Notiere die Zahl hier im Heft und vergleiche diese mit der Zahl an Möglichkeiten bei der herkömmlichen Caesar-Verschlüsselung:

Ein Brechen der Verschlüsselung durch **Brute-Force**, also durch einfaches Durchprobieren aller Möglichkeiten ist in diesem Fall sogar für leistungsstarke Computer nicht in sinnvoller Zeit möglich.

(b) Informiere dich anhand der Schriftstücke in der Truhe über das beschriebene Verfahren und beschreibe kurz in eigenen Worten die Grundidee dieser Technik:

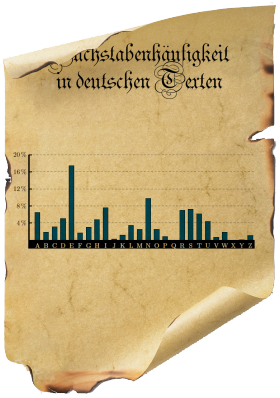
(c) Wende das Verfahren nun auf den Geheimtext an, welcher dadurch „teilentschlüsselt ist“. Gelingt es dir, den gesamten Text zu rekonstruieren? Beschreibe erneut, wie du hierbei vorgegangen bist:

(d) **Geschafft!!** Du hast alle Rätsel im Burghof erfolgreich gemeistert und das erste Teil-Fragment erhalten. Notiere dieses hier im Heft. Auf der nächsten Seite erfährst du noch mehr über die Häufigkeitsanalyse und das Knacken des Vigenère-Verfahrens:



Blättere erst um, wenn du Dein erstes Teil-Fragment erhalten hast!

Überblick (Häufigkeitsanalyse)



Die **Häufigkeitsanalyse** wurde erstmalig von dem arabischen Gelehrten Abu Yusuf Ya qub ibn Ishaq al-Kindi im 8. Jahrhundert in seinem Werk „Abhandlung über die Entzifferung kryptographischer Botschaften“ beschrieben. Hier beschrieb al-Kindi, wie die **monoalphabetische Substitution** (also die Verschlüsselung mit einem Alphabet), die zu dieser Zeit in Europa noch als „unknackbar“ galt, mithilft der statistischen Methode der Häufigkeitsanalyse gebrochen werden konnte. Die entscheidende Passage in al-Kindis Werk lautet:

„Eine Möglichkeit, eine verschlüsselte Botschaft zu entziffern, vorausgesetzt, wir kennen ihre Sprache, besteht darin, einen anderen Klartext in derselben Sprache zu finden, der lang genug ist, um ein oder zwei Blätter zu füllen, und dann zu zählen, wie oft jeder Buchstabe vorkommt. Wir nennen den häufigsten Buchstaben den `ersten`*, den zweithäufigsten den* `zweiten`*, den folgenden den* `dritten` *und so weiter, bis wir alle Buchstaben in der Klartextprobe durchgezählt haben. Dann betrachten wir den Geheimtext, den wir entschlüsseln wollen, und ordnen auch seine Symbole. Wir finden das häufigste Symbol und geben ihm die Gestalt des* `ersten` *Buchstabens der Klartextprobe, das zweithäufigste Symbol wird zum* `zweiten` *Buchstaben, das dritthäufigste zum* `dritten` *Buchstaben und so weiter, bis wir alle Symbole des Kryptogramms, das wir entschlüsseln wollen, auf diese Weise zugeordnet haben.“*

Die Häufigkeitsanalyse wurde im Laufe der Jahrhunderte von Kryptographen und Kryptoanalytikern weiterentwickelt und verfeinert. Beispielsweise kann sie auch zum **Knacken der Vigenère-Verschlüsselung** verwendet werden, was kurz im nachfolgenden Kasten dargestellt wird.

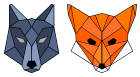
Überblick (Das Knacken des Vigenère-Verfahrens – Der Kasiski-Test)

Der **Kasiski-Test** ist eine Technik, die verwendet wird, um die Schlüssellänge in der Vigenère-Verschlüsselung zu erraten. Dieser Test basiert auf der Beobachtung, dass Wiederholungen von Buchstabenfolgen im Geheimtext auf wiederholte Verwendung des gleichen Schlüsselworts hinweisen können. Der Kasiski-Test basiert dabei auf folgenden Schritten:

(a) **Geheimtext analysieren:** Zuerst wird der Geheimtext sorgfältig analysiert und nach wiederholten Buchstabenfolgen gesucht, die möglicherweise denselben Teil des Klartexts verschlüsseln. Dies sind die Stellen, an denen das Schlüsselwort mehrmals im Geheimtext verwendet wurde.

(b) **Abstandsberechnung:** Für jede gefundene wiederholte Buchstabenfolge wird der Abstand zwischen den Wiederholungen notiert. Der Abstand ist die Anzahl der Buchstaben zwischen den Wiederholungen derselben Buchstabenfolge im Geheimtext.

(c) **Gemeinsame Faktoren finden:** Finde gemeinsame Faktoren zwischen den verschiedenen Abständen. Das bedeutet, dass man nach Abständen sucht, die durch die gleiche Zahl teilbar sind.



Zum Beispiel, wenn die Abstände 6, 12 und 18 sind, haben sie den gemeinsamen Faktor 6. Dies könnte auf die Schlüssellänge hinweisen. Die polyalphabetische Verschlüsselung würde somit aus 6 monoalphabetischen Verschlüsselungen bestehen.

(d) **Häufigkeitsanalyse:** Sobald man eine Schätzung für die Schlüssellänge hat, teilt man den Gesamttext in Abschnitte dieser Länge auf und versucht, jede Gruppe z.B. mit einer Häufigkeitsanalyse zu knacken.

Platz für zusätzliche Notizen: